Notice of Allowability	Application No.	Applicant(s)	
	09/676,748	NUNNS, ANDREW EDWARD	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *October 13, 2005*.

2. ☒ The allowed claim(s) is/are *6-10,13,16-31 and 34-50*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Allowable Subject Matter

1. Claims 6-10,13,16-31 and 34-50 are allowed.

2. The following is an examiner's statement of reasons for allowance:

The primary reasons for the allowance of the independent claims 6, 9, 13,16, 19, 21, 24, 26, 29, 34, 35, 37, 43, 44 and 48 are the inclusion of the following limitations that are not found in the prior art and they are uniquely distinct features. The closest prior arts are Priem et al. (5,652,793; hereinafter Priem), Thompson et al (5,267,312; hereinafter Thompson) and Folmsbee (6,609,201 B1). Priem discloses a method and apparatus for controlling the operation of a computer system. Priem also discloses an encoding circuit that generates a verification value by using a secret key to encode a concatenated value. Thompson discloses a system that it makes difficult for an unauthorized receiver to descramble pre-scrambled entertainment signals. Thompson also discloses that the scrambles signals are transmitted from a head-end to a user receiver that includes a programmable integrated device (PLD) and an authorized mechanism that descrambles the transmitted signals for authorized receivers. Folmsbee teaches a CPU for secure execution of programs that includes a reconfigurable logic circuitry for processing instructions from an instruction buffer included in the microprocessor. However, these three arts singularly or in combination, fail to anticipate or render the following limitations:

"Claims 6 and 13: wherein the encryption operation uses an encryption key to generate a second encrypted bit in the second encrypted data stream from at least the first permuted bit."

"Claim 9: wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream."

"Claims 16: authorization detection circuitry configured to at least periodically compare the first and second encrypted data streams at multiple points during the first time interval and further configured to disable operation of said programmable logic device if the first and second encrypted data streams indicate that said programmable logic device is not authorized to utilize the configuration data during the first time interval."

"Claim 19: wherein said authorization device generates the first encrypted data stream in response to the at least weakly random data stream;

wherein said authorization detection circuitry operates as a dead man switch internal to said programmable logic device; and

wherein each of a plurality of bits in the second encrypted data stream is determined by performing the encryption operation on at least one respective bit in the

first encrypted data stream and at least one respective bit in the at least weakly random data stream."

"Claim 21: authorization detection circuitry that at least periodically compare the first and second time-varying encrypted data streams at multiple points during the first time interval and disables operation of said integrated circuit device if the first and second time-varying encrypted data streams indicate that said integrated circuit device is not authorized to perform the first operations."

"Claim 24: wherein said authorization device generates the first time-varying encrypted data stream in response to the at least weakly random data stream;

wherein said authorization detection circuitry operates as a dead man switch internal to said integrated circuit device; and

wherein each of a plurality of bits in the second time-varying encrypted data stream is determined by performing the encryption operation on at least one respective bit in the first time-varying encrypted data stream and at least one respective bit in the at least weakly random data stream."

"Claim 26: evaluating the first and second time-varying encrypted data streams at least periodically during the first time interval and disabling operation of the programmable logic device during a subsequent second time interval if a comparison of the first and second time-varying encrypted data streams indicate that the

programmable logic device is not authorized to perform the first operations during the first time interval."

"Claim 29: wherein the at least weakly random data stream is generated internal to the programmable logic device;

wherein the at least weakly random data stream is provided by a single wire bus to a device external to the programmable logic device; and

wherein the at least weakly random data stream is time division multiplexed on the bus with the second encrypted data stream."

"Claim 34: wherein each of a plurality of bits within the second data stream is generated within said first integrated circuit component using an encryption operation that is a function of at least one bit in the first data stream and at least one bit in the second data stream."

"Claim 35: wherein a first encrypted bit within the second data stream is generated within said first integrated circuit component using an encryption operation that is a function of at least one bit in the first data stream and a plurality of previously generated encrypted bits in the second data stream."

"Claim 37: a second component that generates the first time-varying data stream provided to said first component and at least periodically evaluates the second time-

varying encrypted data stream received by said second component to assess whether performance of at least one operation within the second component is authorized during a time interval when the first time-varying data stream and the second time-varying encrypted data stream are being generated."

"Claim 43: a second component that at least periodically evaluates the second encrypted data stream to assess whether performance of at least one operation within the second component is authorized during a time interval when the first data stream is being generated; and

wherein said second component comprises circuitry that operates as a deadman switch to disable performance of the at least one operation within said second component if the second and third encrypted data streams fail to indicate that said second component is authorized by said first component to perform the at least one operation."

"Claim 44: said first integrated circuit device having authorization detection circuitry therein that receives and at least periodically evaluates the first and second time-varying data streams at multiple points during the time interval and disables the software and/or hardware controlled operations when the first and second time-varying data streams fail to indicate a sufficient match between said second integrated circuit device and the software and/or hardware controlled operations performed by said first integrated circuit device during the time interval."

"Claim 48: wherein said first integrated circuit device comprises authorization detection circuitry that generates an error history from the first and second encrypted data streams."

3. The dependent claims 7-8, 10, 17-18, 20, 22-23, 25, 27-28, 30-31, 36, 38-42, 45-47 and 49-50 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A.N.

November 25, 2005

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100